## REMARKS

### I. Initial Remarks

Claims 1-20 and 25-32 are pending. Claims 1, 6, 11 and 16 are independent claims. Claims 1, 6, 11, and 16 are amended purely to clarify the address, and no new matter is added. Nor is the claim scope narrowed by the amendment. No claims are new or cancelled. For at least the reasons set forth below, all pending claims are believed to be in condition for allowance.

In the Office Action, claims 1-20 and 25-32 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Pat. No. 6,330,562 B1 to Boden et al. ("Boden"). Applicants respectfully traverse the rejection.

In view of the following arguments, all claims are believed to be in condition for allowance over the references of record. Therefore, this response is believed to be a complete response to the Office Action.[1] Further, for any instances in which the Examiner took Official Notice in the Office Action, Applicants expressly do not acquiesce to the taking of Official Notice, and respectfully request that the Examiner provide an affidavit to support the Official Notice taken in the next Office Action, as required by 37 CFR 1.104(d)(2) and MPEP § 2144.03.

### II. Claim Rejections – 35 U.S.C. § 102

#### A. Independent Claim 1

##### 1. "a translator configured to restore predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include a previously translated address, the previously translated address being

[1] As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine references, assertions as to dependent claims, etc.) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants reserve the right to analyze and dispute such assertions/requirements in the future.

**restored into an address from which the previously translated address was translated"**

Claim 1 recites in part "a translator configured to restore predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include a previously translated address, the previously translated address being restored into an address from which the previously translated address was translated." The Examiner cited col. 5, lines 37-42, col. 6, lines 40-51, and col. 7, lines 58-67 of Boden as allegedly disclosing the recitation. (Office Action, page 3.) However, at most Boden discloses use of "Internet Security Association Key Management Protocol (ISAKMP)" for "maintaining the keys used by the negotiated IPSec protocols." (Boden, col. 4, lines 19-22.) Nowhere does Boden teach or suggest "a translator configured to restore predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key," let alone "wherein the predetermined portions include a previously translated address, the previously translated address being restored into an address from which the previously translated address was translated" as recited by independent claim 1. (Emphasis added.)

Boden discloses "a data model . . . for abstracting customer-defined VPN security policy information," through which "a VPN node (computer system existing in a Virtual Private Network) can gather policy configuration information for itself through a GUI, or some distributed policy source, store this information in a system-defined database, and use this information to dynamically negotiate, create, delete, and maintain secure connections at the IP level with other VPN nodes." (Boden, col. 3, lines 23-32.) Boden states in its background section that "filter rules are written statically with predefined IP selectors (IP addresses, port numbers, and transport protocol). However, when dealing with a dynamically assigned IP address from a third party (such as an Internet Service Provider, or ISP), there is no way currently of knowing what IP address to configure in the rules, particularly for handling different security policies for different hosts (users)." (Boden, col. 2, lines 31-38.) Thus, Boden teaches that

> remote initiating hosts with dynamically assigned IP addresses are handled through the use of deferred selectors. With as little as one anchor filter, connection filter rules can be generated and loaded

> dynamically at negotiation time. Negotiation is performed using a non-IP-type selector, such as user@[Fully Qualified Domain Name (FQDN)], for both phase I and phase II (whereas phase II negotiations are usually performed using IP-type only client IDs). Following successful negotiation and authentication via [Internet Key Exchange], the remote host IP address for the filter rules is determined by the IP packet source address.

(Boden, col. 6, lines 40-51.) With regard to the data model of Boden,

> Each object in a database has a unique key for keyed reference. This key is either a name or an ID, depending or the database. An ID is an identification of a system or group of systems in the VPN (e.g. An FQDN or an IPV4 subnet). All references between objects of different databases is via object name.
>
> All databases in which objects have names support keyed references by object name. All other databases support keyed references by ID (i.e., ID of a specific system or group of systems).

(Boden, col. 7, lines 58-67.) Additionally as cited by the Examiner,

> Manual connection component 12 provides information for manual (i.e., static) security associations (SAs), which information describes such attributes as encryption and authentication procedures, and must be hand coded by the user, with mirror images on both initiator 18 and responder 19 in order for a manual tunnel to work over connection 213.

(Boden, col. 5, lines 37-42.)

Although Boden discusses various aspects of VPNs, IPSec, and ISAKMP, nowhere does Boden explicitly disclose a "packet header." Moreover, nowhere does Boden in any way teach or suggest "predetermined portions of packet header information of a data packet", "wherein the predetermined portions include a previously translated address," and "the previously translated address being restored into an address from which the previously translated address was translated." Additionally, nowhere does Boden teach or suggest any system element or elements "configured to restore predetermined portions of packet header information of a data packet," let alone "a translator configured to restore predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key."

For at least these reasons, Boden fails to teach or suggest the recitation of independent claim 1. Thus, the Examiner's rejection of independent claim 1, as well as all claims depending therefrom, should be withdrawn.

**2. "an actuator configured to trigger a security device when the address does not match an entry in the host table"**

Claim 1 further recites "an actuator configured to trigger a security device when the address does not match an entry in the host table." The Examiner cited col. 6, lines 13-31 of Boden as disclosing the recitation. (Office Action, page 4.) However, at most the cited section of Boden discloses details relating to phase II of ISAKMP negotiation. Nowhere does Boden teach or suggest "an actuator configured to trigger a security device when the address does not match an entry in the host table" as recited by claim 1.

The cited portion of Boden states that

> In accordance with the preferred embodiment of the invention, previously unknown client ID pairs (IDci and IDcr values) are accepted from a remote system. The user writes as few as one filter rule (also referred to as an anchor rule) for the subset of IP traffic to be protected, similar to conventional filter rules. However, this anchor filter rule, by way of its association with a connection definition, is not explicit about what future security associations (SAs) will be used to protect any of the traffic defined by the anchor rule. It only specifies things like what policy to negotiate and what granularity of client IDs to accept. Connection filters are generated and loaded dynamically based on either locally defined connections (user client pair objects 52), IDci/IDcr from a remote system, or from an IP packet (for on demand connections). If a remote system offers client IDs of, say, only TCP traffic between the local host and a given subnet, connection filters for that traffic only would be generated and loaded, with all other traffic between the local host and the given subnet discarded.

(Boden, col. 6, lines 13-31.) However, disclosure of filter rules specifying "things like what policy to negotiate and what granularity of client IDs to accept" fails to teach or suggest the recitation of claim 1. Although Boden discloses that "previously unknown client ID pairs . . . are accepted from a remote system," nowhere does Boden teach or suggest "an actuator" and "a security device," let

alone "an actuator configured to trigger a security device when the address does not match an entry in the host table" as recited by claim 1.

For at least these additional reasons, Boden fails to teach or suggest the recitation of independent claim 1. Thus, the Examiner's rejection of independent claim 1, as well as all claims depending therefrom, should be withdrawn.

**B. Independent Claims 6, 11, and 16**

Applicants submit that independent claims 6, 11, and 16 are patentable over Boden at least for reasons similar to those set forth above regarding independent claim 1.

Independent claim 1 recites "a translator configured to restore predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include a previously translated address, , the previously translated address being restored into an address from which the previously translated address was translated." Independent Claim 6 includes the similar recitation "restoring predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include a previously translated address, the previously translated address being restored into an address from which the previously translated address was translated." As another example, claim 1 recites "an actuator configured to trigger a security device when the address does not match an entry in the host table," and claim 6 recites "triggering a security device when the address does not match an entry in the host table." Although claim 6 is a method claim and recites different details than the apparatus of claim 1, Boden lacks the requisite teachings.

Similarly, independent claim 11 recites in part "means for restoring predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include a previously translated address, the previously translated address being restored into an address from which the previously translated address was

translated" and "means for triggering a security device when the address does not match an entry in the host table." Although claim 11 is a means plus function claim and claim 1 recites an apparatus, for similar reasons as discussed above with regard to claim 1, Boden fails to teach or suggest these recitations of claim 11 as well.

Moreover, independent claim 16 recites in part "[a] bastion host adapted for processing packet header information of a data packet." Nowhere does Boden teach or suggest "a bastion host" as recited by claim 16. Additionally, claim 16 further recites "restore predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include a previously translated address, the previously translated address being restored into an address from which the previously translated address was translated" and "trigger a security device when the address does not match an entry in the host table." As discussed above with regard to claim 1, although claim 16 recites a bastion host adapted for processing packet header information of a data packet and different details, Boden lacks the required teachings.

Accordingly, for at least the foregoing reasons, claims 6, 11, and 16 are patentable over Boden and Applicants respectfully request that the Examiner withdraw the rejection of these claims, which also are in condition for allowance.

### C. Dependent Claims 2-5, 12-15, 17-20, And 25-32

Claims 2-5, 12-15, 17-20, and 25-32 are in condition for allowance at least because they are dependent from one of independent claims 1, 6, 11 or 16. Further, the dependent claims also recite independently patentable subject matter, representative examples of which are discussed below.

#### 1. Claim 2, 7, 12, And 17

Claim 2 recites in part "wherein the security device is a logging device configured to log the data packet." The Examiner cited col. 8, lines 15-67 of Boden as allegedly disclosing the recitation. (Office Action, page 4.) However, the cited portion of Boden states that "[in] accordance with the

preferred embodiment of the model, the following databases are provided," and then lists the included fields for various databases. (Boden, col. 8, lines 15-67.) For example, Boden discloses a "deferred selectors 22 database" including a "name field." As another example, Boden discloses a "static authorization header security association (SA) pairs database 46" including "name, inbound and outbound IPSec security policy indices (SPIs)." (Id.) However, none of the database definitions disclose a field including logged data packets, let alone a "logging device configured to log the data packet." Moreover, a listing of databases and included fields in no way teaches or suggests "to log the data packet," let alone "wherein the security device is a logging device configured to log the data packet" as recited by claim 2. For at least these reasons, claim 2 is separately patentable.

Moreover, claim 7 recites in part "logging the data packet when the address does not match an entry in the host table." (Emphasis added.) Claim 12 recites in part "means for logging the data packet when the address does not match an entry in the host table." Claim 17 recites in part "the bastion host being further operable to log the data packet when the address does not match an entry in the host table." (Emphasis added.) The Examiner did not specifically cite any reference as allegedly disclosing these recitations, and instead indicated that these claims are rejected according to the previous rejections of claims 1-5 and 25-26. (Office Action, page 5.) However, as discussed above, Boden lacks the requisite disclosure. Thus, for at least the reasons discussed above with regard to claim 2, claims 7, 12, and 17 are separately patentable.

### 2. Claims 3, 8, 13, And 18

Claim 3 recites in part "wherein the security device is configured to signal an alarm when triggered." The Examiner cited col. 11, lines 38-54 of Boden as allegedly disclosing the recitation. (Office Action, page 4.) The cited section of Boden states

> A series of 'integrity checks' or audits are performed on the data in the VPN Policy database to ensure correct operation of the VPN. These audits may be done either during policy creation and updating, or during runtime, when the data is acted upon. These audits include general audits and audits specific to a database. General audits include (a) ensuring objects referenced by other objects exist, (b)

> fields are valid, (c) object is unique with respect to its key (name or ID), and (d) indicated protocols and algorithms are supported.

(Boden, col. 11, lines 38-54.) However, disclosure of performing audits on a VPN Policy database with regard to the data integrity of the database in no way teaches or suggests the recitation of claim 3. Simply nowhere does Boden teach or suggest "wherein the security device is configured to signal an alarm when triggered." For at least these reasons, claim 3 is separately patentable.

Moreover, claim 8 recites in part "signaling an alarm when the security device is triggered." Claim 13 recites in part "means for signaling an alarm when the security device is triggered." Claim 18 recites in part "the bastion host being further operable to signal an alarm when the security device is triggered." The Examiner did not specifically cite any reference as allegedly disclosing these recitations, and instead indicated that these claims are rejected according to the previous rejections of claims 1-5 and 25-26. (Office Action, page 5.) However, as discussed above, Boden lacks the requisite disclosure. Thus, for at least the reasons discussed above with regard to claim 3, claims 8, 13, and 18 are separately patentable.

### 3. Claims 25-32

Claim 25 recites in part "wherein the address includes a network portion and an apparatus portion, the apparatus portion of the address having been translated without the network portion also being translated, and wherein said translator is configured to restore the apparatus portion of the address without also restoring the network portion of the address." The Examiner cited col. 6, lines 32-39 as allegedly disclosing the recitation. (Office Action, page 5.) The cited section of Boden states

> Further in accordance with the preferred embodiment of the invention, ISAKMP phase II driven phase I connections are enabled. That is, a phase I connection is only created or refreshed if there is an active phase II connection that requires it. This reduces unnecessary IKE traffic. Also, phase I security policy and other attributes are based solely on the remote endpoint and not on the phase II traffic being ultimately protected, thus easing setup and policy definition.

(Boden, col. 6, lines 32-39.) However, general disclosure regarding the two phases ISAKMP negotiation in no way teaches or suggests the recitations of claim 25. For example, nowhere does Boden teach or suggest "wherein the address includes a network portion and an apparatus portion." Moreover, nowhere does Boden teach or suggest "the apparatus portion of the address having been translated without the network portion also being translated," and "and wherein said translator is configured to restore the apparatus portion of the address without also restoring the network portion of the address." For at least these reasons, claim 25 is separately patentable.

Moreover, claim 26 recites in part "wherein the data packet includes a translated packet header with a plurality of fields carrying packet header information, the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header, and wherein said translator is configured to restore at least a portion of the packet header information in the one or more predetermined fields." The Examiner cited the same section of Boden (i.e., col. 6, lines 32-39) as allegedly disclosing this recitation as well. (Office Action, page 5.) However, general disclosure of the two phases of ISAKMP negotiation in no way teaches or suggests the recitations of claim 26. For example, nowhere does Boden in any way teach or suggest "the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header." (Emphasis added.) For at least these reasons, claim 26 is separately patentable.

Claims 27, 29, and 31 each includes recitations similar to the recitation of claim 25. Additionally, claims 28, 30, and 32 each includes recitations similar to the recitation of claim 26. The Examiner did not specifically cite any reference as allegedly disclosing the recitation of claims 27-32, and instead indicated that these claims are rejected according to the previous rejections of claims 1-5 and 25-26. (Office Action, page 5.) However, as discussed above, Boden lacks the requisite disclosure. Thus, for at least the reasons discussed above with regard to claims 25 and 26, claims 27-32 are separately patentable.

## CONCLUSION

In view of the above amendment, Applicants believe the pending application is in condition for allowance.

Applicants believe no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-0013, under Order No. 65632-0534 from which the undersigned is authorized to draw. To the extent necessary, a petition for extension of time under 37 C.F.R. § 1.136 is hereby made, the fee for which should be charged to this deposit account.

Dated: January 21, 2009

Respectfully submitted,

Electronic signature: /Michael B. Stewart/
Michael B. Stewart
Registration No.: 36,018
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 25537
Attorney for Applicant